UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/656,634	09/07/2000	Babak Tehranchi	81399N-R	1654

1333 7590 04/15/2005

PATENT LEGAL STAFF
EASTMAN KODAK COMPANY
343 STATE STREET
ROCHESTER, NY 14650-2201

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 04/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/656,634	TEHRANCHI, BABAK	
	Examiner	Art Unit	
	Benjamin E Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47 and 50-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47 and 50-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 07 February 2005 amends claims 11-6, 47, 52, 53, 57, and cancels claims 48, 49, 59-61. Applicant's amendment has been fully considered and is entered.

Response to Arguments

2. Applicant's arguments filed 07 February 2005 have been fully considered but they are not persuasive. Applicant's argument that the Warren reference does not disclose block synchronization data is not persuasive because Figure 12 shows explicitly that each data block contains the encryption key for the frame contained in the next data block.

3. Applicant's argument that the Warren reference does not disclose synchronization data that associates each data block with a distinct encryption key is not persuasive because Warren discloses that each data block contains the key for the next data block (Fig. 12), which further meets the limitation of providing an identifier that correlates a mapping algorithm to said plurality of encryption keys.

4. Applicant's argument that there is no motivation to combine the teaching of Warren and Shukla is not persuasive because it would have been obvious to one of ordinary skill in the art at the time the invention was made for the data blocks of Warren to be different sizes in order to avoid the use of many standard techniques used in encryption methods as taught in Shukla (Col. 2, lines 48-53).

5. Applicant's argument that the Warren reference does not disclose the type of frames set forth in claim 52 is not persuasive because Warren discloses intra-coded frames being encrypted (Col. 3, lines 8-27)

6. Applicant's argument that the Warren reference does not disclose the data blocks containing an offset value is persuasive a new grounds of rejection follows under Warren in view of Rump.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1, 2, 4-10, 13, 15, 16, 28, 30, 32-36, 38-41, 43, 44, 52, 58 are rejected under 35 U.S.C. 102(e) as being anticipated by Warren, U.S. Patent No. 5,963,909. Referring to claims 1, 28, 30, 32, 34, 58, Warren discloses a copy management system for multi-media wherein multi-media data is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56), which meets the limitation of partitioning the digital motion image data stream into a plurality of digital motion image data blocks, an encryption key generator for providing an encryption key assigned to each single data block of the plurality of data blocks. Figure 12 shows explicitly that each data block contains the encryption key for the frame contained in the next data block, which meets the limitation of block synchronization index indicating a correspondence between said encryption key and single data block. Figure 12 shows a multi-media data stream that has been encrypted with the corresponding keys (Col. 13, line 58 – Col. 14, line 3), which meets the limitation of an encryption engine that, for each said single data block, produces an encrypted

data block using said encryption key fro said encryption key generator. The multi-media data stream is transmitted over a data channel (Col. 2, lines 27-34), which meets the limitation of a data transmission channel for delivering said encryption data block from said encryption engine to the digital data receiver. The multi-media data stream could include a plurality of data channels, with one of the data channels including the encryption key data (Col. 2, lines 27-34), which meets the limitation of a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver. As specified above, the encryption key data also provides the means for the block synchronization as disclosed in Figure 12, which meets the limitation of a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver.

Referring to claims 2, 39, Warren discloses that the receiver contains a decryption engine (Fig. 17) to decrypt the encrypted multi-media stream with the encryption keys that are embedded in the stream (Fig. 12, Col. 13, line 58 – Col. 14, line 3), which meets the limitation of digital receiver includes a decryption engine which is responsive to said encryption key and said encryption engine and decryption engine are provided with symmetric encryption, the encrypted data blocks comprise digital motion image data blocks and the digital motion image data blocks are decrypted by providing a digital motion image data frame or digital motion image data frame component identification; and generating a corresponding key from the plurality of encryption keys for use in decrypting the block of which the frame or frame component forms a part.

Referring to claims 4, 40, 41, Warren discloses that the multi-media data is video (Abstract).

Referring to claim 5, Warren discloses that the communication channel can be a satellite channel (Col. 1, lines 22-24), which meets the limitation of the data transmission channel being a wireless transmission network.

Referring to claim 6, Warren discloses that the communication channel can be a telephone network (Col. 6, line 40), which meets the limitation of a data transmission channel that utilizes dedicated phone service.

Referring to claims 7, 13, 16, Warren discloses that the communication network uses a portable storage medium (Col. 1, lines 10-15).

Referring to claims 8-10, Warren discloses that the communication network can be cable networks, The Internet, or intranets (Col. 1, lines 22-23), which meets the limitation of a computer data network, wide area network and a local area network.

Referring to claim 15, Warren discloses that the channel that the encryption keys are distributed on can be encrypted (Col. 16, lines 16-24 & Fig. 12).

Referring to claims 17, 43, Warren discloses that the data can be compressed (Col. 2, lines 31-33), which meets the limitation of single data block is compressed.

Referring to claims 33, 35, Warren discloses that the encrypted data is recorded on a medium (Fig. 15, 140).

Referring to claim 36, Warren discloses a copy management system for multi-media wherein multi-media data is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56). The multi-media data stream could include a plurality of data channels, with one of the data channels including the encryption key data (Col. 2, lines 27-34), which meets the

limitation of providing said plurality of encryption keys separately from said encrypted data blocks. Figure 12 shows explicitly that each data block contains the encryption key for the frame contained in the next data block, which meets the limitation providing an identifier that correlates a mapping algorithm to said plurality of encryption keys.

Referring to claim 38, Warren discloses that NULL keys can be used to created unencrypted data blocks (Col. 14, lines 18-21), which meets the limitation of padding said plurality of encryption keys using dummy bits.

Referring to claim 44, Warren discloses that the compression can be done using MPEG compression methods (Col. 5, line 4).

Referring to claim 52, Warren discloses that the receiver contains a decryption engine (Fig. 17) to decrypt the encrypted multi-media stream with the encryption keys that are embedded in the stream (Fig. 12, Col. 13, line 58 – Col. 14, line 3), which meets the limitation of digital receiver includes a decryption engine which is responsive to said encryption key and said encryption engine and decryption engine are provided with symmetric encryption, the encrypted data blocks comprise digital motion image data blocks and the digital motion image data blocks are decrypted by providing a digital motion image data frame or digital motion image data frame component identification; and generating a corresponding key from the plurality of encryption keys for use in decrypting the block of which the frame or frame component forms a part. Warren discloses that the compression can be done using MPEG compression methods (Col. 5, line 4).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

11. Claims 3, 20-25, 27, 29, 47, 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Rump, U.S. Patent No. 6,735,311. Referring to claims 3, 20, 29, 47, 57, Warren discloses a copy management system for multi-media wherein multi-media data is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56), which meets the limitation of an encryption key generator for providing an encryption key assigned to each single data block of the plurality of data blocks. Figure 12 shows explicitly that each data block contains the encryption key for the frame contained in the next data block, which meets the limitation of block synchronization index indicating a correspondence between said encryption key and single data block. Figure 12 shows a multi-media data stream that has been encrypted with the corresponding keys (Col. 13, line 58 – Col. 14, line 3), which meets the limitation of an encryption engine that, for each said single data

block, produces an encrypted data block using said encryption key fro said encryption key generator. The multi-media data stream is transmitted over a data channel (Col. 2, lines 27-34), which meets the limitation of a data transmission channel for delivering said encryption data block from said encryption engine to the digital data receiver. The multi-media data stream could include a plurality of data channels, with one of the data channels including the encryption key data (Col. 2, lines 27-34), which meets the limitation of a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver. As specified above, the encryption key data also provides the means for the block synchronization as disclosed in Figure 12, which meets the limitation of a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver. Warren does not disclose having different size data blocks identified by an offset value. Rump discloses a system for encryption and decryption of multi-media data wherein each block contains a block size index (Col. 7, line 18), which meets the limitation of the size of said single data block is further conditioned by an offset value, the size of each successive data block is based on an average size and based on randomly generated offset. The block size indexes can be different corresponding to different sizes (Col. 7, lines 18-35). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the variable block sizes in the multi-media copy management system of Warren in order to simplify and streamline multi-media data processing as taught in Rump (Col. 7, lines 18-35).

Referring to claim 21, Warren discloses that the encrypted data is recorded on a medium (Fig. 15, 140).

Referring to claim 22, Warren discloses that the medium is floppy disks or magnetic tapes (Col. 1, lines 27-28), which meets the limitation of magnetic storage technology.

Referring to claim 23, Warren discloses that the medium is a CD of DVD (Col. 1, lines 13-15), which meets the limitation of an optical medium.

Referring to claim 24, Warren discloses the multi-media data stream is transmitted over a data channel (Col. 2, lines 27-34), which meets the limitation of providing said encrypted data block comprises the step of transmitting said encrypted data block to the digital data receiver.

Referring to claim 25, Warren discloses that the channel that the encryption keys are distributed on can be encrypted (Col. 16, lines 16-24 & Fig. 12).

Referring to claim 27, Warren discloses that the multi-media data is video (Abstract), which meets the limitation of digital motion image data.

Referring to claim 51, Warren discloses that the data can be compressed (Col. 2, lines 31-33), which meets the limitation of single data block is compressed.

12. Claims 11, 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Handelman, U.S. Patent No. 5,774,546. Referring to claims 11, 14, Warren discloses a copy management system for multi-media wherein multi-media data is encrypted with a series of encryption keys before being distributed. Each block of the data is encrypted with an encryption for that specific block (Fig. 13, Col. 14, lines 43-56), which meets the limitation of an encryption key generator for providing an encryption key assigned to each single data block of the plurality of data blocks. Figure 12 shows explicitly that each data block contains the encryption key for the frame contained in the next data block, which meets the limitation of block synchronization index indicating a correspondence between said

encryption key and single data block. Figure 12 shows a multi-media data stream that has been encrypted with the corresponding keys (Col. 13, line 58 – Col. 14, line 3), which meets the limitation of an encryption engine that, for each said single data block, produces an encrypted data block using said encryption key fro said encryption key generator. The multi-media data stream is transmitted over a data channel (Col. 2, lines 27-34), which meets the limitation of a data transmission channel for delivering said encryption data block from said encryption engine to the digital data receiver. The multi-media data stream could include a plurality of data channels, with one of the data channels including the encryption key data (Col. 2, lines 27-34), which meets the limitation of a key transmission channel for delivering said encryption key from said encryption key generator to the digital data receiver. As specified above, the encryption key data also provides the means for the block synchronization as disclosed in Figure 12, which meets the limitation of a block synchronization data channel for delivering said block synchronization index from said encryption key generator to the digital data receiver. Warren does not disclose using smart cards in the copy management system. Handelman discloses a data access system wherein video data is accessed using a smart card that communicates seeds, keys, and access control algorithms with the video decoder (Col. 2, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use smart cards in the copy management system of Warren in order to provide secure access to restricted means as taught in Handelman (Col. 1, line 18).

13. Claims 12, 18, 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909. Referring to claim 18, Warren discloses that the system can use a number of different associations between the encryption keys and the data frames (Col. 3, lines

18-27), but Warren does not disclose that this association is chosen randomly. It would have been obvious to one of ordinary skill in the art at the time the invention was made to randomly choose the association between the encryption keys and the data frames in order to make the copy protection harder to break.

Referring to claims 12, 31, Warren does not disclose that this association is encrypted, but it would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt this association between the encryption keys and the data frames in order to shield this security association, that is necessary for copy protection, from would be pirates.

14. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Schneier. Referring to claim 19, Warren does not disclose that linear feedback shift registers can randomly generate the associations. Schneier discloses that pseudo-random sequences can be generated using linear feedback shift registers (Page 373). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the pseudo-random sequences of Warren to be generated using a linear feedback shift register because shift registers have been used to generate stream ciphers since the beginning of electronics as taught in Schneier (Page 372).

15. Claims 26, 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Dahan, U.S. Patent No. 6,137,763. Referring to claims 26, 37, Warren discloses that data is stored on optical mediums (Col. 1, lines 13-15) and transferred sequentially (Fig. 13) as opposed to non-sequentially. Dahan discloses a method of buffering data read from an optical disk wherein the data is read from the disk in a non-sequential order (Col. 2, lines 32-42). It would have been obvious to one of ordinary skill in the art at the time the

invention was made for the data of Warren to be transmitted in non-sequential order because Dahan discloses that non-sequential reads of optical disks occur, and would therefore need a correctional mechanism to insure that correct sequencing occurs. It would be obvious to eliminate this correction step to lower production costs and processing time.

16. Claims 42, 45, 46, 50, 53-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren, U.S. Patent No. 5,963,909, in view of Chaum, U.S. Patent No. 5,959,717. Referring to claims 42, 50, Warren does not disclose that the video signal can be decoded at a projector. Chaum discloses a copy protection system that utilizes two video parts in combination at the projector to view the film (Col. 1, line 46 – Col. 2, line 54). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the decoder of Warren to be housed in a projector because film projection systems are the dominate way to publicly screen motion pictures as taught in Chaum (Col. 1, lines 12-14).

Referring to claims 45, 46, 53-56, Warren does not disclose that the video signal is encrypted based on color data. Chaum discloses that rather than performing frame by frame protection of the film, protection can be performed on a color basis (Col. 5, lines 14-17). It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the video data of Warren with respect to color in order to produce holes in the video content so that theft or piracy would be less desirable as taught in Chaum (Col. 5, lines 16-30).

Conclusion

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th0 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100